RCA PF030097AC

CITED BY APPLICANT

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
7 mars 2002 (07.03.2002)

PCT

(10) Numéro de publication internationale
WO 02/19613 A1

(51) Classification internationale des brevets[7] : H04L 9/32

(21) Numéro de la demande internationale :
PCT/FR01/02720

(22) Date de dépôt international : 31 août 2001 (31.08.2001)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
00/11142 31 août 2000 (31.08.2000) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **CP8 TECHNOLOGIES** [FR/FR]; 68, route de Versailles, BP 45, F-78431 Louveciennes Cedex (FR).

(72) Inventeur; et

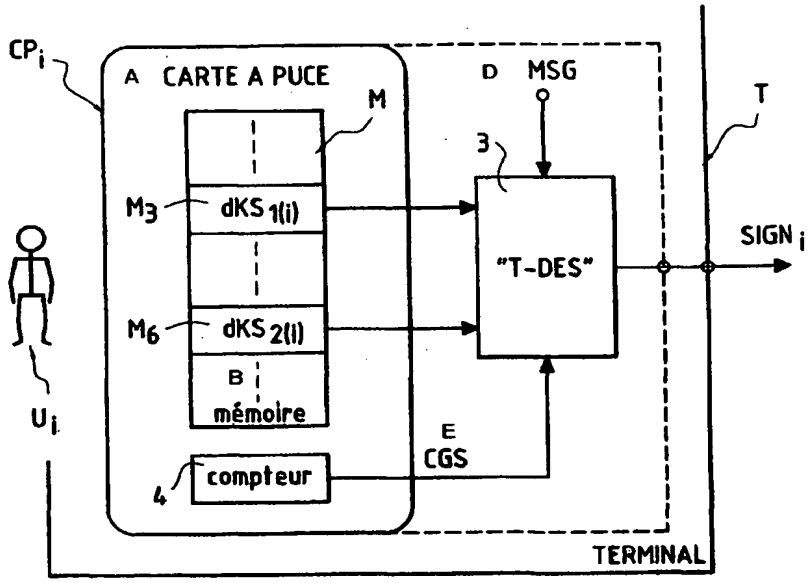
(75) Inventeur/Déposant *(pour US seulement)* : **HAZARD, Michel** [FR/FR]; 27, rue des Harias, F-78124 Mareil-sur-Mauldre (FR).

(74) Représentant commun : **RENAULT, Patricia**; CP8 Technologies, Direction de la Propriété Intellectuelle, 36-38, rue de la Princesse - BP 45, F-78431 Louveciennes Cedex (FR).

[Suite sur la page suivante]

(54) Title: METHOD FOR GENERATING UNCHALLENGEABLE SIGNATURES, IN PARTICULAR BY AN INTEGRATED SYSTEM, AND INTEGRATED SYSTEM THEREFOR

(54) Titre : PROCEDE DE GENERATION DE SIGNATURES NON-REPUDIABLES, NOTAMMENT PAR UN SYSTEME EMBARQUE, ET SYSTEME EMBARQUE POUR LA MISE EN OEUVRE DU PROCEDE



A... SMART CARD
B... STORAGE
4... COUNTER
D... MESSAGE TO BE SIGNED
T... HOST TERMINAL
E... SIGNATURE GENERATION COUNTER

(57) **Abstract:** The invention concerns a method for generating unchallengeable signature with a smart card *(CP_i)*. The latter stores in a storage unit *(M)*two pairs of so-called mother keys and two diversified keys *($dKS_{1(i)}$ and $dKS_{2(i)}$)* obtained from said pair of keys and an identifier, by applying a triple DES cryptographic algorithm and a certificate generated by a certification authority based a private key of said authority, a public key and by applying a RSA cryptographic algorithm. The signature*($SIGN_i$)* is obtained from the two diversified keys *($dKS_{1(i)}$ and $dKS_{2(i)}$)* and data *(MSG)* to be transmitted by applying a triple DES (3). In a preferred embodiment, two authenticating additional keys are stored in the storage unit (M). Said keys are generated by the certification authority and serve to generate data authenticating the signature, by applying a triple DES.

[Suite sur la page suivante]

WO 02/19613 A1

(81) États désignés *(national)* : AU, BR, CA, CN, JP, KR, NO, SG, US.

(84) États désignés *(régional)* : brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Publiée :

— *avec rapport de recherche internationale*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : L'invention concerne un procédé de génération de signature non-répudiable par une carte à puce (CP_i). Celle-ci stocke dans une mémoire (M) deux paires de clés dites mères et deux clés diversifiées ($dKS_{1(i)}$ et $dKS_{2(i)}$) obtenues à partir de ces paires de clés et d'un identifiant, par application d'un algorithme de cryptographie de type triple "DES" et un certificat généré par une autorité de certification à partir d'une clé privée de cette autorité, d'une clé publique et par application d'un algorithme de cryptographie de type "RSA". La signature ($SIGN_i$) est obtenue à partir des deux clés diversifiées ($dKS_{1(i)}$ et $dKS_{2(i)}$) et des données (MSG) à transmettre par application d'un triple "DES" (3). Dans une variante préférée, deux clés supplémentaires d'authentification sont stockées dans la mémoire (M). Ces clés sont générées par l'autorité de certification et servent à générer des données d'authentification de la signature, par application d'un triple "DES".

PROCEDE DE GENERATION DE SIGNATURES NON-REPUDIABLES, NOTAMMENT PAR UN SYSTEME EMBARQUE, ET SYSTEME EMBARQUE POUR LA MISE EN ŒUVRE DU PROCEDE

L'invention concerne un procédé de génération de signatures non répudiables, notamment par un système embarqué à puce électronique.

L'invention concerne encore un système embarqué pour la mise en œuvre du procédé, notamment une carte à puce.

Dans le cadre de l'invention, le terme "système embarqué" doit être compris dans son sens le plus général. Il concerne notamment toutes sortes de terminaux légers munis d'une puce électronique, et plus particulièrement les cartes à puce proprement dites. La puce électronique est munie de moyens d'enregistrement et de traitement de données numériques, par exemple un microprocesseur pour ces derniers moyens.

Pour fixer les idées, et sans que cela limite en quoi que ce soit sa portée, on se placera ci-après dans le cas de l'application préférée de l'invention, à savoir les applications à base de cartes à puce, sauf mention contraire.

Ces dernières années, les échanges de documents sous forme électronique se sont fortement accrus, notamment via le réseau Internet. Or ces échanges posent plusieurs problèmes. En particulier, comme dans le cas de documents sous forme traditionnelle, c'est-à-dire notamment sous forme papier, il est généralement nécessaire d'y apposer une signature et, surtout que cette signature identifie sans ambiguïté l'émetteur du document et ne soit pas répudiable par son destinataire.

Jusqu'à une période récente, seuls les documents "papiers" pouvaient faire foi. Dans beaucoup de pays, la loi exige d'ailleurs une signature manuscrite originale. Or, dans un environnement électronique, l'original d'un document, par exemple d'un contrat, ne se distingue en aucune façon d'une copie.

Il existe cependant des technologies qui permettent de remplir tout ou partie de fonctions perçues comme caractéristiques d'une signature manuscrite traditionnelle. Ces technologies mettent en œuvre généralement

des techniques de chiffrement, associées ou non à des certificats d'authentification. La signature électronique est une séquence binaire habituellement obtenue par le chiffrement du message transmis à l'aide d'un algorithme de cryptologie particulier et de clés de signature. On doit bien comprendre cependant que le message proprement dit peut être transmis en clair s'il n'existe pas de besoins particuliers de confidentialité. Il s'agit d'une technique dite de "scellement". Le message et la signature sont transmis au destinataire, accompagnés éventuellement d'éléments de clés de chiffrement ou de vérification dans certains procédés de cryptographie mettant en œuvre une clé dite publique. Le destinataire utilise la signature et le message transmis à l'aide du même algorithme et la clé publique précitée, ce qui lui permet de vérifier l'authenticité de la signature de l'émetteur. Accessoirement, le processus permet de garantir l'intégrité du message transmis. En effet, si celui-ci venait à être corrompu de façon fortuite ou malveillante, le déchiffrement permet de mettre ce dysfonctionnement en évidence.

Certains pays, comme l'Allemagne, l'Italie, le Danemark, en Europe, certains Etats des Etats-Unis ou du Canada (le Québec) ont légalisé des procédés de signature électronique.

Fin 1999, le Parlement Européen et le Conseil de l'Union Européenne ont émis une directive qui devra être transcrite dans les droits nationaux des pays membres (article 13). Dans l'article premier de cette directive, 1 er alinéa, il est indiqué que "*l'objectif de la présente directive est de faciliter l'utilisation des signatures électroniques et de contribuer à leur reconnaissance juridique. Elle institue un cadre juridique pour les signatures électroniques et certains services de certification afin de garantir le bon fonctionnement du marché intérieur*".

A l'article 2, une "*signature électronique*" est définie comme suit : "*une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification*".

Il est prévu deux types de signatures électroniques, l'une pouvant être qualifiée de "simple". La seconde est appelée "*avancée*" dans la

directive. Il s'agit d'une signature électronique "*qui satisfait aux exigences suivantes :*

a) être liée uniquement au signataire ;

b) permettre d'identifier le signataire ;

c) être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ; et

d) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable".

L'invention vise plus particulièrement le second type de signature électronique. Pour ce faire, il est nécessaire d'avoir recours à des dispositifs sécurisés, mettant en œuvre un procédé de chiffrement (signature) de données, des certificats dits "qualifiés" et une autorité, appelée "*prestataire de service de certification*" dans la directive, que l'on appellera ci-après "autorité de certification". L'autorité de certification génère notamment une clé publique utilisée dans le processus précité par les cartes à puce.

En effet, de façon pratique, des procédés de cryptographie asymétriques doivent être utilisés. Selon ces procédés, il est mis en œuvre une clé de signature privée, c'est-à-dire secrète, détenue par le signataire, et une clé publique de vérification de signature. En réalité, dans les applications à base de carte à puce, la clé privée est enregistrée dans une zone de mémoire non-volatile des cartes à puce du signataire, mémoire de type "ROM", "EEPROM" ou équivalent.

Les procédés de cryptographie asymétriques sont réputés non répudiables car le vérificateur de la signature, du fait des caractéristiques inhérentes à ces procédés, ne sait pas signer.

Pour fixer les idées, un exemple de procédé de cryptographie asymétrique bien connu et largement utilisé est constitué par le procédé dit "RSA" (du nom de ses inventeurs Rivest, Shamir et Adleman). Une description de ce procédé peut être trouvée dans le brevet US-A-4405829.

Bien qu'efficaces, les procédés de cryptographie asymétriques ne sont pas pour autant dépourvus d'inconvénients. Ils sont en effet délicats et coûteux à mettre en œuvre.

En premier lieu, il nécessaire de gérer et générer autant de paires de clés privée/publique qu'il y a d'utilisateurs à doter de cet instrument de signature électronique.

En second lieu, la cryptographie asymétrique nécessite des ressources informatiques non négligeables, du moins par rapport à celles habituellement offertes par une puce électronique. Il est notamment nécessaire de prévoir un co-processeur arithmétique pour effectuer les calculs de chiffrement/déchiffrement.

Il s'ensuit que le coût de puces électroniques dotées de la puissance de calcul nécessaire à la cryptographie asymétrique est sensiblement plus élevé que les puces traditionnelles utilisées à ce jour par l'ensemble des autres applications. Or, les considérations de coût, pour un composant de très grande diffusion, sont primordiales.

On pourrait penser avoir recours à des procédés de cryptographie symétrique, moins exigeants en ressources informatiques. Cependant ces derniers, de par leurs caractéristiques propres, ne peuvent garantir la condition de "non répudiabilité" recherchée, car le vérificateur de la signature peut également signer, puisqu'il se trouve *a priori* dans les mêmes conditions que le signataire.

L'invention vise à pallier les inconvénients des procédés et dispositifs de l'art connu, dont certains viennent d'être rappelés, tout en satisfaisant aux besoins qui se font sentir.

L'invention se fixe pour but un procédé de génération de signatures non répudiables, spécialement adapté à des applications mettant en œuvre des terminaux légers tels des systèmes embarqués à puce électronique, et plus particulièrement des cartes à puce, dont l'une des caractéristiques est d'offrir des ressources informatiques limitées.

Pour ce faire, selon une caractéristique avantageuse, le procédé selon l'invention associe la cryptographie symétrique à la cryptographie asymétrique statique, étant entendu que les opérations mettant en œuvre ce dernier procédé ne sont pas effectuées dans le terminal embarqué. Il

s'ensuit qu'il n'est pas nécessaire de doter celui-ci d'une puissance de calcul accrue, notamment d'y implanter un co-processeur mathématique.

Dans un premier mode de réalisation de l'invention, le procédé comprend une phase préliminaire comportant les étapes principales suivantes :

1. On dote toutes les cartes à puce de deux paires de clés de signature dites "mères", les deux paires de clés étant identiques pour toutes les cartes à puce.
2. Chacune des cartes à puce reçoit également deux clés diversifiées propres à chaque carte à puce, calculées à partir de ces paires de clés "mères " et d'un identifiant propre à la carte à puce en question (et/ou de toute autre information identifiant le porteur) et contenu dans celle-ci. Le calcul des clés diversifiées est effectué en ayant recours à un procédé de cryptographie symétrique, de préférence, mais non exclusivement, en faisant appel au procédé dit "triple DES" (pour "Data Encryption Standard").
3. L'identifiant (et éventuellement d'autres informations) de la carte à puce, est(sont) certifié(s) par une clé privée (c'est-à-dire secrète) détenue par une autorité dite de "certification". Ce certificat accompagne l'identifiant dans la carte à puce et constitue "l'habilitation à signer" du porteur de la carte à puce. Le certificat est calculé en ayant recours à un procédé de cryptographie de type asymétrique, de préférence le procédé dit "RSA" précité. Il doit cependant bien être compris que les calculs nécessaires sont effectués par l'autorité de certification, qui peut disposer de moyens informatiques puissants et non par la carte à puce. De façon plus précise, le certificat est calculé à partir des données d'identification de la carte à puce et/ou de son porteur à l'aide d'une clé privée, cette dernière étant propriété de l'autorité de certification.

Dans les applications à base de cartes à puce, cette phase préliminaire est habituellement réalisée lors de l'opération dite de "personnalisation" des cartes à puce.

La clé publique de certification est disponible pour le contrôle des certificats par l'autorité de certification et pour le contrôle par chacun des possesseurs d'un instrument de signature. Ce peut être, dans une première variante de réalisation, l'ensemble des usagers possesseurs d'une carte à puce, ou, dans une seconde variante de réalisation, seulement les usagers appartenant à un même groupe. Dans ce dernier cas, la population des usagers est scindée en au moins deux groupes distincts.

L'algorithme "DES" précité a été publié en 1977 par un organisme officiel américain, le "NBS" ("National Bureau of Standards"). A titre d'exemple, une description de cet algorithme peut être trouvée dans l'article de Jean-Pierre TUAL, intitulé "Cryptographie", paru dans "Les Techniques de l'Ingénieur", volume H2, pages 248-1 à 248-29.

De même, un exemple de mise en œuvre de certificats est décrit dans l'article de Gérard RIBIERE, intitulé "Certification électronique et sécurité", paru "Les Techniques de l'Ingénieur", volume H2, pages 258-1 à 258-11.

Les étapes ultérieures, que l'on pourra qualifier d'opérationnelles, comprennent au moins la génération d'une signature lors de l'émission d'un message ou plus généralement d'un document électronique par l'un des possesseurs de carte à puce, que l'on appellera signataire.

Le calcul de la signature est réalisé par un chiffrement des données à transmettre à l'aide des clés diversifiées précitées, en faisant appel à un algorithme de cryptographie symétrique, de préférence le triple "DES" comme indiqué précédemment.

La reconstitution et la vérification de la signature, s'effectuent par une opération identique au chiffrement, par un ou plusieurs destinataires, à l'aide des clés diversifiées du signataire, reconstituées par le ou les destinataires(s), et du même algorithme symétrique. Le signataire transmet également son certificat et les données d'identification ayant servies à le calculer à l'étape 3.) de la phase préliminaire. Ce certificat est vérifié par le ou les destinataire(s) à l'aide de la clé publique précitée. Il est fait appel à un algorithme asymétrique. Les calculs nécessaires peuvent être effectués par un terminal hôte de la carte à puce.

Selon un deuxième mode de réalisation du procédé selon l'invention, celui-ci comprend également l'essentiel des étapes de la phase préliminaire. Cependant, l'une des deux clés diversifiées est obtenue à partir d'une des deux paires de clés "maître" et de données d'identification d'un destinataire, et non plus de l'émetteur comme dans la première variante. Selon cette variante, seul ce destinataire est alors en mesure de vérifier la signature de l'émetteur. A cette exception près, la vérification s'effectue de la même manière que précédemment.

On constate que, dans ces deux modes de réalisation, toutes les cartes à puce possèdent les deux paires de clés mères, ce qui peut présenter une faiblesse d'un point de vue sécurité.

Aussi, dans une variante préférée, compatible avec les deux modes de réalisation, de manière à augmenter la robustesse du procédé, on ajoute dans chacune des cartes à puce une paire de clés diversifiées issues de la diversification de deux paires de clés d'authentification appartenant à l'autorité de certification. Cette opération est réalisée lors d'une étape supplémentaire de la phase préliminaire. Le calcul des clés de chaque carte à puce est effectué en faisant appel à un algorithme symétrique et à un identifiant propre à cette carte à puce. Comme précédemment, l'algorithme symétrique est préférentiellement un triple "DES". A partir des clés diversifiées résidentes dans la carte à puce et de la signature précédemment générée, en faisant appel à un algorithme symétrique, la carte à puce génère des données supplémentaires que l'on appellera ci-après "données d'authentification de signature". Ces données sont également transmises au(x) destinataire(s). Ce (ces) dernier(s) peu(ven)t les soumettre à l'autorité de certification qui peut à son tour les authentifier par retour.

Dans une variante de réalisation préférée encore, on prévoit avantageusement un compteur de génération de signatures utilisé pour sécuriser la génération de signature et assurer la traçabilité, par exemple pour détecter des signatures différentes portant le même numéro. Les compteurs sont également résidents dans les cartes à puce et peuvent servir optionnellement à l'initialisation de toute signature de données.

L'invention a donc pour objet principal un procédé de génération de signature non-répudiable par une première entité d'un ensemble, notamment par un système embarqué à puce électronique comportant au moins des moyens de mémoire non-volatile et des moyens de calcul, ladite signature étant destinée à être diffusée et vérifiée par au moins l'une desdites entités de l'ensemble, caractérisé en ce qu'il comprend une phase préliminaire comportant au moins les étapes suivantes :

- le stockage dans lesdits moyens de mémoire non-volatile de deux paires de clés de signature dites "mères", communes à toutes lesdites entités ;
- la génération, à partir d'au moins une desdites paires de clés de signature "mères" et d'un identifiant unique, propre à ladite première entité, d'une première clé de signature dite "diversifiée", par application d'un algorithme de cryptographie symétrique et le stockage de ladite clé diversifiée dans lesdits moyens de mémoire non-volatile ;
- le stockage dudit identifiant unique dans lesdits moyens de mémoire non-volatile ;
- la génération par une entité supplémentaire dite "autorité de certification" d'un certificat constituant une habilitation à signer pour ladite première entité, ledit certificat étant obtenu à partir d'au moins ledit identifiant et d'une clé privée de chiffrement détenue par ladite autorité de certification, par application d'un algorithme de cryptographie asymétrique, et le stockage dudit certificat dans lesdits moyens de mémoire non-volatile ; et
- la distribution, par ladite autorité de certification, d'une clé publique de vérification de signature à tout ou partie desdites entités de l'ensemble,

et une phase subséquente comprenant au moins les étapes suivantes :

- la génération de ladite signature non-répudiable à partir de ladite première clé de signature diversifiée, d'une deuxième clé de signature diversifiée et de données à transmettre destinées à au moins une

desdites entités de l'ensemble, par application d'un algorithme de cryptage symétrique ; et

- la diffusion à destination d'au moins l'une desdites entités de l'ensemble d'au moins desdites données, de ladite signature, dudit identifiant et dudit certificat.

L'invention a encore pour objet un système embarqué à puce électronique pour la mise en œuvre de ce procédé, notamment une carte à puce.

L'invention va maintenant être décrite de façon plus détaillée en se référant aux dessins annexés, parmi lesquels :

- la figure 1 illustre schématiquement l'architecture d'une carte à puce pour la génération d'une signature non répudiable selon l'invention ;
- La figure 2 illustre schématiquement la génération d'une clé de signature dite diversifiée pour la carte à puce de la figure 1 à partir d'une paire de clés de signature dites "mères" et d'un identifiant de la carte à puce ;
- la figure 3 illustre schématiquement le processus de génération d'une signature non répudiable selon un premier mode de réalisation du procédé selon l'invention ;
- la figure 4 illustre schématiquement le processus de génération de clés dites d'authentification de signature par une entité dite autorité de certification ;
- la figure 5 illustre schématiquement le processus de génération d'une signature non répudiable selon un deuxième mode de réalisation du procédé selon l'invention ;
- la figure 6 illustre le processus de génération de données dites d'authentification à partir des clés d'authentification et de la signature précitée ;
- la figure 7 illustre schématiquement les différentes données transmises par une carte à puce signataire ;

- la figure 8 illustre schématiquement l'étape de vérification d'une signature générée selon le premier mode de génération de signatures non répudiables ;
- la figure 9 illustre schématiquement l'étape de vérification d'une signature générée selon le deuxième mode de génération de signatures non répudiables ; et
- la figure 10 illustre schématiquement le processus d'authentification par l'autorité précité de certification d'une signature générée par une carte à puce.

On va maintenant décrire de façon plus détaillée un exemple de réalisation préférée de procédé de génération de signatures non répudiables selon l'invention, selon plusieurs variantes.

Comme il a été indiqué, pour fixer les idées, sans limiter en quoi que ce soit la portée de l'invention, on se placera dans le cas d'une application à base de cartes à puce. La puce électronique de cette dernière comprend, de façon habituelle, des moyens de calcul, comprenant par exemple un microprocesseur, et des moyens de mémoire, vive et non-volatile. Une telle architecture est bien connue de l'homme de métier et il est inutile de la décrire plus avant.

La figure 1 illustre schématiquement l'architecture d'une carte à puce CP_i, i étant un indice arbitraire repérant une des cartes à puce d'un ensemble de n cartes à puce CP_1 à CP_n (non représenté). Sur la figure 1, seule la mémoire non-volatile, repérée M, a été représentée. Il peut s'agir d'une mémoire de type "ROM" ("Read-Only Memory", à lecture seule), d'une mémoire de type "EEPROM" (Electrically Erasable Programmable Read Only Memory", à lecture seule, mais re-programmable) ou de toute autre mémoire d'un type similaire.

Lors d'une phase préliminaire, avantageusement lors de la phase dite de "personnalisation" de la carte à puce CP_i, on enregistre, dans des positions de mémoire prédéterminées, M_1, M_2, M_4 et M_5, respectivement dans l'exemple décrit, deux paires de clés dites "mères", MKS_{11} et MKS_{12}, d'une part, et MKS_{21} et MKS_{22}, d'autre part. Ces clés "mères" sont communes à toutes les cartes à puce, CP_1 à CP_n.

Selon une première variante de réalisation du procédé conforme à l'invention, un usager U_i, c'est-à-dire le porteur de la carte à puce CP_i, signe un message ou des données transmises. Tous les autres usagers peuvent vérifier cette signature.

Pour ce faire, deux clés diversifiées, $dKS_{1(i)}$ et $dKS_{2(i)}$, respectivement, sont calculées et enregistrées dans des positions de mémoires, M_4 et M_6, par exemple. Ce calcul, réalisé à l'extérieur de la carte à puce CP_i, met en œuvre un algorithme symétrique. De façon préférentielle, il s'agit d'un triple "DES". On supposera d'ailleurs ci-après, à chaque fois que l'on aura recours à un algorithme symétrique, qu'il s'agit également du triple "DES", que l'on notera ci-après "T-DES" par simplification.

La figure 2 illustre schématiquement le calcul de la clé $dKS_{1(i)}$. Le triple "DES", référencé 1, comprend trois étages en cascade 10 à 12. A titre d'exemple, les étages 10 et 12 réalisent un "DES" dit "direct". La clé de signature utilisée pour ces deux étages est, toujours dans l'exemple, la clé MKS_{11}. L'étage intermédiaire 11 réalise un "DES" dit inverse, que l'on notera "DES^{-1}". La clé de signature utilisée pour cet étage est la clé MKS_{12}. En entrée du premier étage 10, on injecte une donnée d'identification ID_i de la carte à puce CP_i et/ou de son porteur U_i (figure 1). Cette donnée d'identification ID_i peut être unique ou issue de plusieurs données distinctes, par exemple concaténées, avec éventuellement des données de remplissage pour obtenir un mot binaire de longueur prédéterminée. Sur la figure 1, on a représenté deux sources de données d'identification, notées *Info* et *Div* (numéro de la carte à puce CP_i, etc.). Ces données sont également résidentes dans la carte à puce CP_i et, dans l'exemple illustré, enregistrées dans les positions M_7 et M_8 de la mémoire M.

La sortie de l'étage 10 est transmise à l'entrée de l'étage 11 et la sortie de l'étage 11 est transmise à l'entrée de l'étage 12. Finalement, en sortie de l'étage 12, on obtient la clé diversifiée $dKS_{1(i)}$, propre à la carte à puce CP_i, clé diversifiée enregistrée dans la position de mémoire M_3 comme il a été indiqué.

Les calculs s'effectuent en milieu sécurisé, par exemple par une entité que l'on appellera "l'encarteur", en dehors de la carte à puce CP_i. Le module 1 pour la mise en œuvre du "T-DES" peut être indifféremment de type "matériel" (circuits spécialisés) ou faire appel à un logiciel.

La clé $dKS_{2(i)}$ est obtenue de façon identique et il est inutile de re-décrire le processus.

Si on se réfère de nouveau à la figure 1, outre ces différentes données, un certificat CTA_i est calculé par une autorité dite de certification *CA*. Pour ce faire, cette dernière entité *CA* met en œuvre, selon un des aspects du procédé selon l'invention, un algorithme asymétrique, référencé 2, préférentiellement l'algorithme "RSA" précité. Des données d'identification ID_i de la carte à puce CP_i sont chiffrées à l'aide d'une clé privée, propriété de l'autorité de certification *CA*, que l'on notera K_A.

Dans l'exemple illustré par la figure 1, le résultat de l'opération de chiffrement, c'est-à-dire le certificat CTA_i est enregistré dans la position de mémoire M_9.

L'autorité de certification *CA* distribue également une clé publique de vérification de signature, associée à la clé privée K_A et que l'on appellera ci-après K_P, à toutes les cartes à puce.

On a supposé, jusqu'à ce point de la description, que tous les usagers U_i possesseurs d'une carte à puce CP_i faisait partie d'un seul et unique groupe, et donc que la clé publique K_P était mise à la disposition de tous ces usagers U_i. Selon une autre variante du mode de réalisation du procédé, il est possible de scinder l'ensemble de ces usagers en au moins deux groupes (non représentés). Chaque groupe aura donc à sa disposition une clé publique distincte de celle des autres groupes : K_{p1}, K_{p2}, ...,K_{pm}, si on suppose que *m* est le nombre de groupes distincts.

La figure 3 illustre schématiquement la génération d'une signature, référencée $SIGN_i$, par la carte à puce CP_i.

On suppose que le porteur U_i de la carte CP_i veuille envoyer un message *MSG* qui doit être signé. Pour ce faire, le message *MSG* élaboré par des moyens de traitement de données connus, par exemple le terminal hôte *T* de la carte à puce CP_i, est transmis en entrée d'un "T-DES",

référencé 3, ou de tout autre algorithme symétrique similaire. De façon connue en soi, le message *MSG* peut être soumis au préalable à une opération dite de "hachage" ("hashing"). L'architecture logique de ce "T-DES" 3 est identique ou pour le moins tout à fait similaire à celle décrite en regard de la figure 2. La clé utilisée pour les étages "DES" directs est, par exemple, la clé $dKS_{1(i)}$ et la clé utilisée pour l'étage "DES^{-1}" est la clé $dKS_{2(i)}$. Puisqu'il s'agit d'un algorithme symétrique, il n'est pas nécessaire de disposer de moyens de calcul puissants. Le calcul de la signature peut donc s'effectuer avantageusement à l'intérieur de la carte à puce CP_i, à l'aide des moyens de calculs standards dont elle dispose (non représentés). Il s'ensuit que, bien que pour des raisons de clarté du dessin, les moyens de calcul 3 aient été représentés sur la figure à l'extérieur de la carte à puce CP_i, on doit bien comprendre qu'ils sont préférentiellement implantés dans la puce électronique de celle-ci. De façon pratique, il ne s'agit pas habituellement de circuits spécifiques. On préfère effectuer le calcul de la signature $SIGN_i$ à l'aide d'un logiciel, enregistré dans la mémoire *M*, coopérant avec les moyens de calcul standards précités.

On constate que les clés diversifiées, $dKS_{1(i)}$ et $dKS_{2(i)}$, c'est-à-dire le secret propre à chacune des cartes à puce CP_i, ne sont pas dévoilées au monde extérieur. Cependant, toutes les cartes à puce CP_i possèdent les deux paires de clés de signature sous leur forme dite "mère". Si on arrive à "casser" ces clés, la sécurité globale du procédé est mise en péril. Aussi, pour "durcir" le procédé vis-à-vis d'attaques extérieures, on ajoute dans chacune des cartes à puce CP_i une paire de clés de signature diversifiées supplémentaires, que l'on notera $dKSA_{1(i)}$ et $dKSA_{2(i)}$, respectivement. Ces clés sont elles-mêmes issues de la diversification de deux paires de clés d'authentification de signature appartenant à l'autorité de certification *CA* (figure 1). On explicitera ci-après, de façon plus détaillée, l'utilité de ces clés.

La figure 4 illustre schématiquement le processus de génération des clés diversifiées supplémentaires, $dKSA_{1(i)}$ et $dKSA_{2(i)}$. Les paires de clés dites "d'authentification de signature", $MKSA_{11}$ et $MKSA_{12}$, $MKSA_{21}$ et $MKSA_{22}$, respectivement, sont transmises aux entrées de clé de modules mettant en œuvre un algorithme symétrique, préférentiellement un "T-DES",

notés 1' et 1". En entrée de données, on injecte un identifiant ID_i caractérisant la carte à puce CP_i. Le processus de calcul des clés $dKSA_{1(i)}$ et $dKSA_{2(i)}$ est identique, ou pour le moins tout à fait similaire à celui (figure 2 : 1) ayant permis de calculer les clés diversifiées $dKS_{1(i)}$ et $dKS_{2(i)}$. On peut utiliser d'ailleurs les mêmes circuits, s'il s'agit de circuits électroniques spécifiques, ou le même logiciel.

Comme pour les clés diversifiées, $dKS_{1(i)}$ et $dKS_{2(i)}$, le calcul est effectué lors d'une phase préliminaire, en milieu sécurisé, par exemple lors de la phase dite de "personnalisation" de la carte à puce CP_i. Les résultats des calculs, c'est-à-dire les clés d'authentification de signature $dKSA_{1(i)}$ et $dKSA_{2(i)}$, sont enregistrés également dans la mémoire M de la carte à puce, dans les positions M_{10} et M_{11} (voir également la figure 1).

Selon cette variante préférée du procédé, percer le secret d'une carte à puce CP_i devient alors aussi difficile que d'obtenir la clé privée d'une carte à puce qui serait dotée d'un algorithme de cryptographie asymétrique dynamique.

Dans une variante encore du procédé de génération de signature, on prévoit avantageusement un compteur de génération de signature 4, dont la sortie est notée *CGS*. Le compteur 4 est utilisé pour sécuriser la génération de signature et pour assurer la traçabilité (signatures différentes portant le même numéro). Si on se reporte de nouveau à la figure 3, on constate que la sortie *CGS* est transmise à l'entrée de données du "T-DES" 3. De façon pratique, il s'agit d'un mot binaire qui peut être concaténé avec le message à signer *MSG*. Ce compteur 4 est également implanté dans la carte à puce CP_i et sert optionnellement à initialiser toute signature de données. Il peut s'agir d'un composant matériel, appartenant par exemple aux circuits des moyens de calcul de la puce électronique de la carte à puce CP_i. Le comptage (mot *CGS*) peut également être obtenu par des moyens logiciels.

On va maintenant décrire schématiquement un deuxième mode de réalisation du procédé de génération de signature par référence à la figure 5. Selon ce mode de réalisation, une des clés diversifiées, par exemple la clé, référencée désormais $dKS'_{2(i)}$, est obtenue à l'aide des données de

diversification d'une autre carte à puce, du groupe auquel appartient la carte à puce CP_I s'il existe plusieurs groupes distincts, par exemple les données d'identification ID_J de la carte à puce CP_J, et non à partir des données d'identification ID_I de la carte à puce signataire CP_I.

A l'exception de cette caractéristique, les autres phases et étapes sont identiques à celles qui ont été décrites pour le premier mode de réalisation. Il est donc inutile de les re-décrire en entier. De même, ce mode de réalisation est compatible avec l'utilisation de clés d'authentification de signature, $dKSA_{1(I)}$ et $dKSA_{2(I)}$, et avec l'utilisation d'un compteur de génération de signatures 4 produisant le mot *CGS*.

Selon ce mode de réalisation, du fait précisément de la caractéristique précitée, seul le destinataire U_J, c'est-à-dire le possesseur de la carte à puce CP_J est en mesure de vérifier la signature de l'émetteur U_I, notée $SIGN'_I$ sur la figure 5. Il est intéressant de noter que cette dernière caractéristique n'est pas offerte par les procédés classiques de cryptographie asymétrique dynamique utilisés pour la génération de signatures non-répudiables selon l'art connu.

On suppose que, comme précédemment, la clé diversifiées $dKS_{1(I)}$ a été calculée et enregistrée dans la mémoire *M* de la carte à puce CP_I, à la position M_3, lors de la phase préliminaire. Pour ce faire, des données d'identification ID_I propres à la carte à puce CP_I ont été utilisées.

La clé de signature diversifiée $dKS'_{2(I)}$ est calculée à partir de la paire de clés de signature "mères" MKS_{21} et MKS_{22}, comme précédemment, mais en faisant usage de l'identifiant ID_J provenant de la carte à puce CP_I, identifiant enregistré dans une ou plusieurs positions de la mémoire M' de celle-ci, de façon analogue à l'identifiant ID_I pour la carte à puce CP_I. Le calcul de la clé de signature s'effectue en faisant usage d'un "T-DES", référencé 3', recevant sur ces entrées de clé, les clés mères MKS_{21} et MKS_{22}, et, en entrée de données, l'identifiant ID_J précité. La sortie représente la clé de signature diversifiée $dKS'_{2(I)}$.

Lors de l'étape de génération de signature, référencée désormais $SIGN'_I$, le processus mis en œuvre est identique à celui du calcul de la signature $SIGN_I$ de la figure 3. Pour ce faire, on recourt à un algorithme

symétrique, de préférence l'algorithme "T-DES" (module 3), à l'exception du fait que la clé $dKS'_{2(j)}$ est calculée différemment, comme il vient d'être montré. En entrée de données, on injecte le message à signer *MSG*, et optionnellement le mot de comptage de signature *CGS* (compteur 4 : figure 3).

Dans ce mode de réalisation, il est nécessaire d'obtenir un identifiant certifié du destinataire.

Il est à noter que le calcul de signature $SIGN'_i$ est réalisé *a priori* dans la carte à puce CP_i, de manière à ce que les clés diversifiées $dKS_{1(j)}$ et $dKS'_{2(j)}$ restent confinées dans celle-ci. Il en est de même pour le calcul de la clé $dKS'_{2(j)}$ par le module 3'.

Il est à noter également que, dans les deux modes de réalisation, la diversification des paires de clés mères MKS_{11}, MKS_{12}, MKS_{21}, et MKS_{22} par l'identifiant d'une carte à puce, ID_i de la carte à puce CP_i par exemple, qui permettrait de retrouver les clés diversifiées est interdite. Ceci peut être obtenu simplement par des moyens matériels ou logiciels interdisant la divulgation de ces clés et leur mise en œuvre pour la génération d'une signature. Seule la signature obtenue en utilisant ces clés diversifiées peut être transmise au monde extérieur.

Selon les deux modes de réalisation, il est possible de générer des données dites "d'authentification" de la signature émise. La figure 6 illustre schématiquement la génération de telles données, référencées $ASIGN_i$ pour la carte à puce CP_i.

Pour ce faire, on utilise les clés diversifiées supplémentaires dites d'authentification, $dKSA_{1(j)}$ et $dKSA_{2(j)}$, générées de la manière explicitée en regard de la figure 4 et qui sont enregistrées dans la mémoire *M*, dans les positions M_{10} et M_{11}, dans l'exemple décrit. La signature générée $SIGN_i$ est transmise à l'entrée d'un "T-DES", référencé 3". De façon optionnelle, la donnée de comptage *CGS* (figure 3) peut également être injectée en entrée de données, par exemple en la concaténant avec le message à signer *MSG*. Les clés $dKSA_{1(j)}$ et $dKSA_{2(j)}$ sont utilisées comme clés de signature. L'architecture logique du module 3" est identique ou pour le moins tout à fait similaire à celle du module 3 de la figure 3 utilisé pour générer la signature

$SIGN_i$. La sortie du module 3" représente les données d'authentification de signature recherchées $ASIGN_i$. Ces données sont transmises au(x) destinataire(s) de la signature $SIGN_i$. Comme précédemment, le calcul s'effectue à l'intérieur de la carte à puce CP_i pour que les clés $dKSA_{1(i)}$ et $dKSA_{2(i)}$ ne sortent pas de celle-ci. En réalité, le destinataire final des données $ASIGN_i$ est l'autorité de certification CA (figures 1 ou 4). En effet, comme il le sera montré ci-après, un destinataire, par exemple U_j, qui veut faire authentifier la signature reçue $SIGN_i$ et s'assurer que c'est une carte à puce valide CP_i qui l'a émise, soumet les données d'authentification de signature $ASIGN_i$ à l'autorité de certification CA qui seule peut les valider puisqu'elle stocke les clés mères, $MKSA_{11}$ à $MKSA_{22}$, qui ont servi à calculer les clés $dKSA_{1(i)}$ et $dKSA_{2(i)}$.

La figure 7 illustre schématiquement les différentes données transmises par une carte à puce signataire CP_i au(x) destinataire(s), dans une variante de réalisation préférée.

Les données transmises sont les suivantes :

- données ou messages signés MSG ;
- données optionnelles de comptage de signature CGS ;
- signature $SIGN_i$;
- identifiant ID_i de la carte à puce CP_i et/ou de son détenteur U_i ;
- certificat CTA_i, et
- données d'authentification $ASIGN_i$.

C'est à partir de toutes ces données que le ou les destinataire(s) peu(ven)t vérifier la signature $SIGN_i$ et, dans la variante préférée, l'authentifier à l'aide des données $ASIGN_i$.

On va maintenant décrire l'étape de vérification de la signature $SIGN_i$ émise par une carte à puce, par exemple la carte à puce CP_i, ce selon les deux modes principaux de réalisation du procédé qui viennent d'être décrits.

La figure 8 illustre schématiquement l'étape de vérification de la signature $SIGN_i$, générée conformément au premier mode de réalisation du procédé selon l'invention, par au moins un usager U_i appartenant à un groupe donné ou à l'ensemble des usagers, s'il n'existe pas de groupes

distincts. On doit rappeler que le premier mode de réalisation autorise la vérification *a priori* par tous les usagers, U_1 à U_n, à l'écoute du message émis *MSG* et de sa signature $SIGN_i$.

La vérification consiste à reconstituer la signature de l'émetteur et de la comparer à celle reçue. Pour fixer les idées, on considère le cas d'une carte à puce CP_j recevant de la carte à puce CP_i les différentes données illustrées sur la figure 7. L'architecture de la carte à puce CP_j est, *a priori*, tout à fait semblable à celle de la carte à puce CP_i, sinon identique. Celle-ci comprend notamment une mémoire non-volatile référencée M' dans laquelle sont enregistrés les deux paires de clés mères, MKS_{11} à MKS_{22} (positions de mémoire M'_1, M'_2, M'_4 et M'_5), deux clés diversifiées, $dKS_{1(j)}$ et $dKS_{2(j)}$ (positions de mémoire M'_3 et M'_6), secret de la carte CP_j, des données d'identification ID_j (Info' et Div', positions de mémoire M'_7 et M'_8), un certificat CTA_j (position de mémoire M'_9) et, dans une variante préférée, deux clés d'authentification $dKSA_{1(j)}$ et $dKSA_{2(j)}$ (positions de mémoire M'_{10} et M'_{11}).

Une première clé diversifiée, référencée dKS_1 est calculée à partir des clés mères MKS_{11} et MKS_{12} et de l'identifiant ID_i reçu de la carte à puce CP_i, en faisant appel à un algorithme symétrique, préférentiellement un "T-DES", référencé 5*a*. L'identifiant ID_i est injecté sur l'entrée de données. Les clés mères MKS_{11} et MKS_{12} sont transmises aux entrées de clés. Une deuxième clé diversifiée est calculée de la même façon à l'aide du "T-DES" 5*b*, à partir des clés mères MKS_{21} et MKS_{22} et également de l'identifiant reçu ID_i. Les clés diversifiées calculées, dKS_1 et dKS_2, peuvent être stockées temporairement dans des registres, 6*a* et 6*b*, ou dans des positions d'une mémoire vive (non représentée) dont est munie habituellement une carte à puce. Un troisième "T-DES", référencé 5*c* reçoit en entrées de clés les clés calculées précédemment et sur son entrée de données, le message *MSG* transmis par la carte à puce CP_i, ainsi qu'éventuellement le mot de comptage de génération de signatures *CGS*. La donnée en sortie du module 5c, référencée *SIGN*, est supposée représenter la signature $SIGN_i$ émise par la carte à puce CP_i. Les données correspondantes peuvent être stockées dans un registre 6*c* ou une position

de mémoire vive. On prévoit une opération de comparaison effectuée par le module 7. Si la signature reconstituée *SIGN* est identique à la signature reçue $SIGN_i$, le résultat (signal ou données sur la sortie *S*) est positif et cette dernière authentique.

La carte à puce CP_j reçoit également de la carte à puce CP_i le certificat CTA_i (voir figure 7). Ce dernier peut être vérifié par le module 8 à l'aide de la clé publique K_P émise par l'autorité de certification *CA* (figures 1 et 4). Comme il a été rappelé, la clé publique K_P est mise à la disposition de tous les utilisateurs U_j, au moins à l'intérieur d'un même groupe s'il existe plusieurs groupes distincts. Une donnée de vérification du certificat CTA_i est disponible sur la sortie *S'*.

Pour des raisons de clarté du dessin, les "T-DES", 5*a* à 5*c*, les registres, 6*a* à 6*c*, les organes de comparaison 7 et de vérification 8 ont été représentés à l'extérieur de la carte à puce CP_j. Il va de soi que, comme précédemment, ces derniers sont implantés dans la carte à puce, les clés diversifiées et les résultats des calculs ne devant pas être divulgués au monde extérieur. Les fonctions réalisées peuvent d'ailleurs faire appel en tout ou partie à des logiciels.

La vérification d'une signature générée conformément au deuxième mode de réalisation du procédé selon l'invention va maintenant être décrite par référence à la figure 9. Les éléments communs aux figures précédentes, notamment à la figure 8, portent les mêmes références et ne seront re-décrits qu'en tant que de besoin.

Comme précédemment, une clé diversifiée, dKS_1, est calculée à partir de l'identifiant ID_i reçu de la carte à puce CP_i. Par contre la clé diversifiée $dKS_{2(j)}$, stockée dans la carte à puce CP_j, est directement utilisée comme clé de signature. On suppose que la clé $dKS_{2(j)}$ a été obtenue par diversification à partir des clés mères MKS_{21} et MKS_{22} et de l'identifiant ID_j fourni par la carte à puce CP_j. La clé $dKS_{2(j)}$ et la clé calculée dKS_1 sont transmises aux entrées de clés du "T-DES" 5*c*, qui reçoit sur son entrée de données, comme précédemment, le message transmis MSG et, optionnellement, le mot de comptage de signature *CSG*. Le reste du

processus est identique à celui décrit pour le premier mode de réalisation (figure 9), et il est inutile de le re-décrire en détail.

Le certificat CTA_i est vérifié de la même façon que précédemment.

Dans les deux cas la signature calculée, *SIGN* n'est jamais délivrée au monde extérieur. Seul le résultat de la comparaison peut être divulgué.

En résumé de ce qui précède, puisque ni les clés diversifiées, secret de chaque carte à puce, par exemple CP_i, ni les résultats des calculs de signature ne sortent des cartes à puce, il s'ensuit que le système est non répudiable.

On va maintenant décrire, par référence à la figure 10, la vérification de l'authenticité de la signature $SIGN_i$.

Tout usager U_j ayant vérifié une signature générée par un autre usager, par exemple U_i, peut soumettre à l'autorité de certification *CA* l'identifiant du signataire ID_i, le certificat de cet identifiant CTA_i, la signature $SIGN_i$, les données d'authentification $ASIGN_i$ et les données optionnelles de comptage de génération de signature *CGS*.

A partir de ces données, l'autorité de certification *CA* recalcule, à partir des paires de clés mères $MKSA_{11}$ à $MKSA_{22}$ et du diversifiant ID_i (après contrôle de l'identité certifiée) de la carte à puce signataire CP_i et/ou de son porteur U_i, des clés diversifiées $dKSA_{1(i)}$ et $dKSA_{2(i)}$, pour contrôler les données d'authentification de signature $ASIGN_i$.

Les paires de clés mères $MKSA_{11}$-$MKSA_{12}$, d'une part, et $MKSA_{21}$-$MKSA_{22}$, d'autre part, sont transmises aux entrées de clés de deux modules "T-DES", 9*a* et 9*b*, qui reçoivent, sur leurs entrées de données, les identifiants ID_i. Les sorties de ces modules fournissent les clés diversifiées d'authentification de signature, $dKSA_{1(i)}$ et $dKSA_{2(i)}$, clés transmises aux entrées de clés d'un troisième "T-DES", référencé 9c. Ce dernier reçoit sur son entrée de données, la signature $SIGN_i$ et les données de comptage de génération de signature optionnelles *CGS*. Les données *ASIGN* présentes sur la sortie du "T-DES" 9*c* sont sensées représenter les données $ASIGN_i$ reconstituées. Elles sont donc comparées à ces dernières dans un module comparateur 9*d*. Le résultat de la comparaison, positif ou négatif, est disponible sur la sortie S" du module 9*d*. Ce résultat est retourné à l'usager

qui en fait la demande, par exemple l'usager U_j, signé par les clés $dKSA_{1(j)}$ et $dKSA_{2(j)}$ et d'un "T-DES" 9*e*. Naturellement, ces clés, $dKSA_{1(j)}$ et $dKSA_{2(j)}$, ne sont pas transmises directement par l'usager U_j, mais recalculées par l'autorité de certification CA, par application de "T-DES" (non représentés) et à l'aide des clés mères $MKSA_{11}$-$MKSA_{12}$, d'une part, et $MKSA_{21}$-$MKSA_{22}$, d'autre part, et de l'identifiant ID_j de l'usager U_j, de façon analogue au calcul des clés $dKSA_{1(j)}$ et $dKSA_{2(j)}$. Le résultat signé R, en sortie du "T-DES" 9*e*, peut alors être déchiffré par l'usager U_j à l'aide de ses propres clés d'authentification $dKSA_{1(j)}$ et $dKSA_{2(j)}$, par application d'un "T-DES" supplémentaire (non représenté).

Optionnellement, un mot de passe ou toute identification analogue ("PIN-code, etc.) peut être exigée pour renforcer encore la sécurité du processus.

A la lecture de ce qui précède, on constate aisément que l'invention atteint bien les buts qu'elle s'est fixés.

Elle assure, notamment dans sa variante de réalisation préférée, une grande sécurité et la possibilité d'obtenir une non-répudiation des signatures émises, ce sans devoir recourir à des procédés de cryptage asymétriques au sein de cartes à puce, et de façon plus générale de terminaux embarqués légers à puce électronique. De ce fait, il devient possible d'utiliser des puces électroniques pourvues de moyens de calcul et de mémoire standards. En particulier, il n'est pas nécessaire que la puce électronique soit pourvue d'un co-processeur mathématique.

Il s'ensuit que le coût et la complexité induits par le procédé restent dans des limites acceptables pour des applications dites "grand public"

Il doit être clair cependant que l'invention n'est pas limitée aux seuls exemples de réalisations explicitement décrits, notamment en relation avec les figures 1 à 10.

En particulier, bien que l'algorithme asymétrique "RSA" et l'algorithme symétrique de type triple "DES" soient particulièrement intéressants, l'invention n'est en aucune façon limitée à ces seuls algorithmes. D'autres algorithmes, tant asymétriques que symétriques, respectivement, sont tout à fait envisageables. Le choix d'un algorithme

particulier ne constitue qu'un choix technologique à la portée de l'Homme de Métier, en fonction notamment de l'application précise visée.

REVENDICATIONS

1. Procédé de génération de signature non-répudiable par une première entité d'un ensemble, notamment par un système embarqué à puce électronique comportant au moins des moyens de mémoire non-volatile et des moyens de calcul, ladite signature étant destinée à être diffusée et vérifiée par au moins l'une desdites entités de l'ensemble, caractérisé en ce qu'il comprend une phase préliminaire comportant au moins les étapes suivantes :

   - le stockage dans lesdits moyens de mémoire non-volatile (M) de deux paires de clés de signature dites "mères" (MKS_{11}-MKS_{12}, MKS_{21}-MKS_{22}), communes à toutes lesdites entités (CP_i, CP_j) ;
   - la génération, à partir d'au moins une desdites paires de clés de signature "mères" (MKS_{11}-MKS_{12}) et d'un identifiant unique (ID_i), propre à ladite première entité (CP_i), d'une première clé de signature dite diversifiée ($dKS_{1(i)}$), par application d'un algorithme de cryptographie symétrique (1) et le stockage de ladite clé diversifiée dans lesdits moyens de mémoire non-volatile (M) ;
   - le stockage dudit identifiant unique (ID_i) dans lesdits moyens de mémoire non-volatile (M) ;
   - la génération par une entité supplémentaire dite "autorité de certification" (CA) d'un certificat (CTA_i) constituant une habilitation à signer pour ladite première entité (CP_i), ledit certificat (CTA_i) étant obtenu à partir au moins dudit identifiant (ID_i) et d'une clé privée de chiffrement (K_A) détenue par ladite autorité de certification (CA), par application d'un algorithme de cryptographie asymétrique (2), et le stockage dudit certificat (CTA_i) dans lesdits moyens de mémoire non-volatile (M) ; et
   - la distribution, par ladite autorité de certification, d'une clé publique de vérification de signature (K_P) à tout ou partie desdites entités (CP_i, CP_j) de l'ensemble

   et une phase subséquente comprenant au moins les étapes suivantes :

- la génération de ladite signature non-répudiable ($SIGN_i$) à partir de ladite première clé de signature diversifiée ($dKS_{1(i)}$), d'une deuxième clé de signature diversifiée ($dKS_{2(i)}$, $dKS'_{2(j)}$) et de données à transmettre (MSG) destinées à au moins une desdites entités (CP_j) de l'ensemble, par application d'un algorithme de cryptage symétrique (3, 3') ; et
- la diffusion à destination d'au moins l'une desdites entités (CP_j) de l'ensemble d'au moins lesdites données (MSG), de ladite signature ($SIGN_i$), dudit identifiant (ID_i) et dudit certificat (CTA_i).

2. Procédé selon la revendication 1, caractérisé en ce que ladite deuxième clé de signature diversifiée ($dKS_{2(i)}$) est générée, pendant ladite phase préliminaire, à partir de ladite deuxième paire de clés de signature "mères" (MKS_{21}-MKS_{22}) et dudit identifiant unique propre (ID_i) à ladite première entité (CP_i), par application d'un algorithme de cryptographie symétrique (1), et en ce que ladite deuxième clé de signature diversifiée ($dKS_{2(i)}$) est stockée dans lesdits moyens de mémoire non-volatile (M).

3. Procédé selon la revendication 1, caractérisé en ce que ladite deuxième clé de signature diversifiée ($dKS'_{2(j)}$) est générée à partir de ladite deuxième paire de clés de signature "mères" (MKS_{21}-MKS_{22}) et d'un identifiant unique (ID_j) propre à l'une desdites entités (CP_j), destinataire de ladite signature non-répudiable ($SIGN_i$), par application d'un algorithme de cryptographie symétrique (3').

4. Procédé selon la revendication 1, caractérisé en ce qu'il comprend une étape supplémentaire de génération, pendant ladite phase préliminaire, par ladite autorité de certification (CA), d'une paire de clés de signature supplémentaires dites d'authentification ($dKSA_{1(i)}$, $dKSA_{2(i)}$) à partir de deux paires de clés de signature dites "mères" ($MKSA_{11}$-$MKSA_{12}$, $MKSA_{21}$-$MKSA_{22}$) propres à cette autorité (CA) et dudit identifiant (ID_i) propre à ladite première entité (CP_i), par application d'un algorithme de chiffrement symétrique (1', 1"), et en ce que ladite paire de clés d'authentification ($dKSA_{1(i)}$, $dKSA_{2(i)}$) est stockée dans lesdits moyens de mémoire non-volatile (M).

5. Procédé selon la revendication 4, caractérisé en ce qu'il comprend une étape de génération, par ladite première entité (CP_i), de données dites d'authentification de signature ($ASIGN_i$) à partir de ladite paire de clés de signature supplémentaires d'authentification ($dKSA_{1(i)}$, $dKSA_{2(i)}$) et d'au moins ladite signature non-répudiable ($SIGN_i$), et en ce que lesdites données d'authentification de signature ($ASIGN_i$) sont diffusées à destination d'au moins une desdites entités (CP_j) de l'ensemble.

6. Procédé selon la revendication 1, caractérisé en ce qu'il comprend une phase de vérification de ladite signature non-répudiable ($SIGN_i$) par au moins une deuxième entité (CP_j) dudit l'ensemble comportant au moins les étapes suivantes :

- la génération de première et seconde clés de signature diversifiées (dKS_1, dKS_2), chacune desdites clés de signature étant générée à partir desdites paires de clés "mères" " (MKS_{11}-MKS_{12}, MKS_{21}-MKS_{22}) stockées dans lesdits moyens de mémoire non-volatile (M) et dudit identifiant (ID_i) diffusé par ladite première entité (CP_i), par application d'un algorithme cryptographie symétrique (5*a*, 5*b*) ;
- la reconstitution d'une signature ($SIGN$), à partir de ces dites clés de signature diversifiées (dKS_1, dKS_2) et d'au moins desdites données (MSG) transmises par ladite première entité (CP_i), par application d'un algorithme de cryptographie symétrique (5*c*) ; et
- la vérification de ladite signature non-répudiable ($SIGN_i$) générée par ladite première entité (CP_i) par comparaison (S, 7) de celle-ci avec ladite signature reconstituée ($SIGN$), de manière à valider lesdites données transmises (MSG).

7. Procédé selon la revendication 6, caractérisé en ce qu'il comprend une étape de vérification (8) dudit certificat (CTA_i) transmis par ladite première entité (CP_i), à l'aide de ladite clé publique de vérification de signature (K_P) délivrée par ladite autorité de certification (CA).

8. Procédé selon la revendication 7, caractérisé en ce que ledit ensemble est partitionné en plusieurs groupes distincts d'entités et en ce que ladite autorité

de certification (*CA*) distribue à chacun desdits groupes une clé publique différente.

9. Procédé selon la revendication 5, caractérisé en ce qu'il comprend une phase de vérification desdites données d'authentification comportant au moins les étapes suivantes :

- la soumission à ladite autorité de certification (*CA*), par au moins l'une desdites entités (CP_j) de l'ensemble, desdites données d'authentification ($ASIGN_i$) reçues de ladite première entité (CP_i) ;
- la génération par ladite autorité de certification (*CA*) de première et seconde clés de vérification diversifiées ($dKSA_1$, $dKSA_2$), chacune desdites clés de vérification étant générée à partir desdites paires de clés "mères" ($MKSA_{11}$-$MKSA_{12}$, $MKSA_{21}$-$MKSA_{22}$) propres à ladite autorité de certification (*CA*) et dudit identifiant (ID_i) diffusé par ladite première entité (CP_i), par application d'un algorithme de cryptographie symétrique (9*a*, 9*b*) ;
- la reconstitution de données d'authentification de signature (*ASIGN*), à partir de ces dites clés de vérification diversifiées générées ($dKSA_1$, $dKSA_2$) et d'au moins ladite signature ($SIGN_i$) transmise par ladite première entité (CP_i), par application d'un algorithme de cryptographie symétrique (9*c*) ; et
- la vérification desdites données d'authentification de signature ($ASIGN_i$), transmises par ladite première entité (CP_i), par comparaison (S", 9d) de celles-ci avec lesdites données d'authentification de signature reconstituées (*ASIGN*), de manière à les valider ; et
- la retransmission du résultat (S") de la comparaison à ladite entité (CP_j) ayant soumis lesdites données d'authentification de signature ($ASIGN_i$).

10. Procédé selon la revendication 4, caractérisé en ce qu'il comprend des étapes de génération (4) de données de comptage de génération de signature (*CSG*) et en ce que lesdites données de comptage de génération de signature (*CSG*) sont utilisées conjointement aux dites données à transmettre (*MSG*)

pour générer ladite signature non- répudiable ($SIGN_i$) et/ou à cette signature ($SIGN_i$) pour générer lesdites données d'authentification de signature ($ASIGN_i$).

11. Procédé selon la revendication 1, caractérisé en ce que lesdits algorithmes de cryptographie symétrique (1, 3) sont constitués par des triples "DES".

12. Procédé de génération de signature non-répudiable par une première entité (CPi) d'un ensemble, notamment par un système embarqué à puce électronique comportant au moins des moyens de mémoire non-volatile et des moyens de calcul, ladite signature étant destinée à être diffusée et vérifiée par au moins l'une desdites entités (CPj) de l'ensemble, caractérisé en ce qu'il consiste à générer ladite signature non-répudiable ($SIGN_i$) à partir d'une première clé de signature diversifiée ($dKS_{1(i)}$) obtenue à partir d'au moins une paire de clés de signature "mères" (MKS_{11}-MKS_{12}) communes à toutes les entités (CPi, CPj) et d'un identifiant unique (ID_i), propre à ladite première entité (CP_i) par application d'un algorithme de cryptographie symétrique (1), d'une deuxième clé de signature diversifiée ($dKS_{2(i)}$, $dKS'_{2(i)}$) et de données à transmettre (MSG) destinées à au moins une desdites entités (CP_j) de l'ensemble, par application d'un algorithme de cryptage symétrique (3, 3'), la signature étant destinée à être diffusée à au moins l'une desdites entités (CP_j) de l'ensemble avec au moins lesdites données (MSG), ledit identifiant (ID_i) et un certificat (CTA_i) constituant une habilitation à signer pour la première entité (CPi) obtenu à partir au moins dudit identifiant (ID_i) et d'une clé privée de chiffrement (K_A) détenue par une autorité de certification (CA), par application d'un algorithme de cryptographie asymétrique (2).

13. Procédé de personnalisation d'une entité (CPi) d'un ensemble dans le but de mettre en œuvre le procédé de génération de signature non-répudiable par ladite entité (CPi) selon la revendication 12, caractérisé en ce qu'il comprend les étapes suivantes :

- le stockage dans lesdits moyens de mémoire non-volatile (M) de deux paires de clés de signature dites "mères" (MKS_{11}-MKS_{12}, MKS_{21}-MKS_{22}), communes à toutes lesdites entités (CP_i, CP_j) ;

- la génération, à partir d'au moins une desdites paires de clés de signature "mères" (MKS_{11}-MKS_{12}) et dudit identifiant unique (ID_i), propre à ladite première entité (CP_i), de ladite première clé de signature diversifiée ($dKS_{1(i)}$), par application d'un algorithme de cryptographie symétrique (1) et le stockage de ladite clé diversifiée dans lesdits moyens de mémoire non-volatile (M) ;
- le stockage dudit identifiant unique (ID_i) dans lesdits moyens de mémoire non-volatile (M) ;
- le stockage dans lesdits moyens de mémoire non-volatile (M) dudit certificat (CTAi) généré par une entité supplémentaire dite "autorité de certification" (CA) constituant une habilitation à signer pour ladite première entité (CP_i), ledit certificat (CTA_i) étant obtenu à partir au moins dudit identifiant (ID_i) et de ladite clé privée de chiffrement (K_A) détenue par ladite autorité de certification (CA), par application d'un algorithme de cryptographie asymétrique (2).

14. Système embarqué à puce électronique destiné à la génération d'une signature non-répudiable destinée à être diffusée et vérifiée par au moins un deuxième système embarqué d'un ensemble, chacun desdits systèmes embarqués comprenant au moins des moyens de mémoire non-volatile et des moyens de calculs implantés dans ladite puce électronique, caractérisé en ce que lesdits moyens de mémoires non-volatile (M) stockent au moins deux paires de clés de vérification dites "mères" (MKS_{11}-MKS_{12}, MKS_{21}-MKS_{22}), un identifiant (ID_i) propre au dit système embarqué (CP_i), au moins une première clé de vérification dite "diversifiée" ($dKS_{1(i)}$), générée à partir d'une desdites paires de clés de vérification "mères" (MKS_{11}-MKS_{12}) et dudit identifiant (ID_i), par application d'un algorithme de cryptographie symétrique (1), et un certificat (CTA_i), généré par une entité dite "autorité de certification" (CA) à partir d'une clé privée de signature (K_A) détenue par ladite autorité de certification (CA) et dudit identifiant (ID_i), par application d'un algorithme de cryptographie asymétrique (2), et en ce qu'il comprend des moyens de génération (1) de ladite signature par application d'un algorithme de cryptographie symétrique (3, 3'), en faisant usage de ladite première clé de signature diversifiée ($dKS_{1(i)}$), d'une seconde clé de signature diversifiée ($dKS_{2(i)}$, $dKS'_{2(i)}$) et de données à diffuser et

à signer (*MSG*), pour transmission à destination d'au moins un deuxième système embarqué (CP_j) dudit ensemble.

15. Système selon la revendication 14, caractérisé en ce que lesdits moyens de mémoire (*M*) stockent en outre une paire de clés de vérification supplémentaires dites d'authentification ($dKSA_{1(i)}$, $dKSA_{2(i)}$), générées par ladite autorité de certification (*CA*) à partir d'une paire de clés de vérification dites "mères" ($MKSA_{11}$-$MKSA_{12}$, $MKSA_{21}$-$MKSA_{22}$) propres à cette autorité de certification (*CA*) et dudit identifiant (ID_i) propre à ladite première entité (CP_i), par application d'un algorithme de chiffrement symétrique (1', 1").

16. Système selon la revendication 14, caractérisé en ce qu'il est constitué par une carte à puce (CP_i).

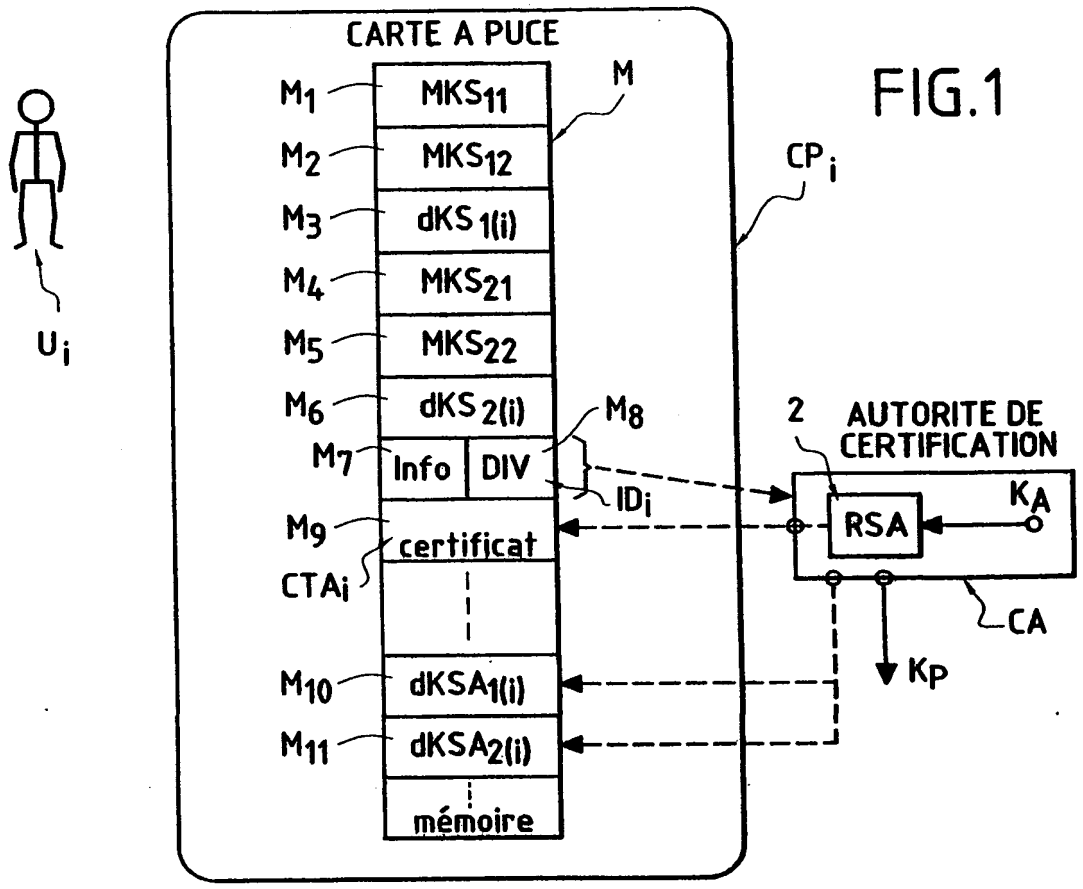
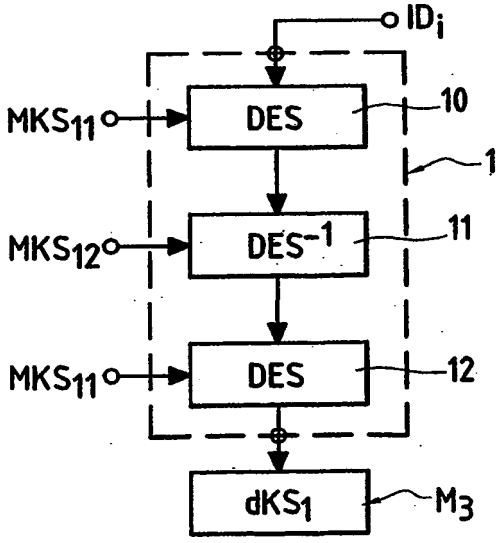


FIG.1



Triple "DES"

FIG.2

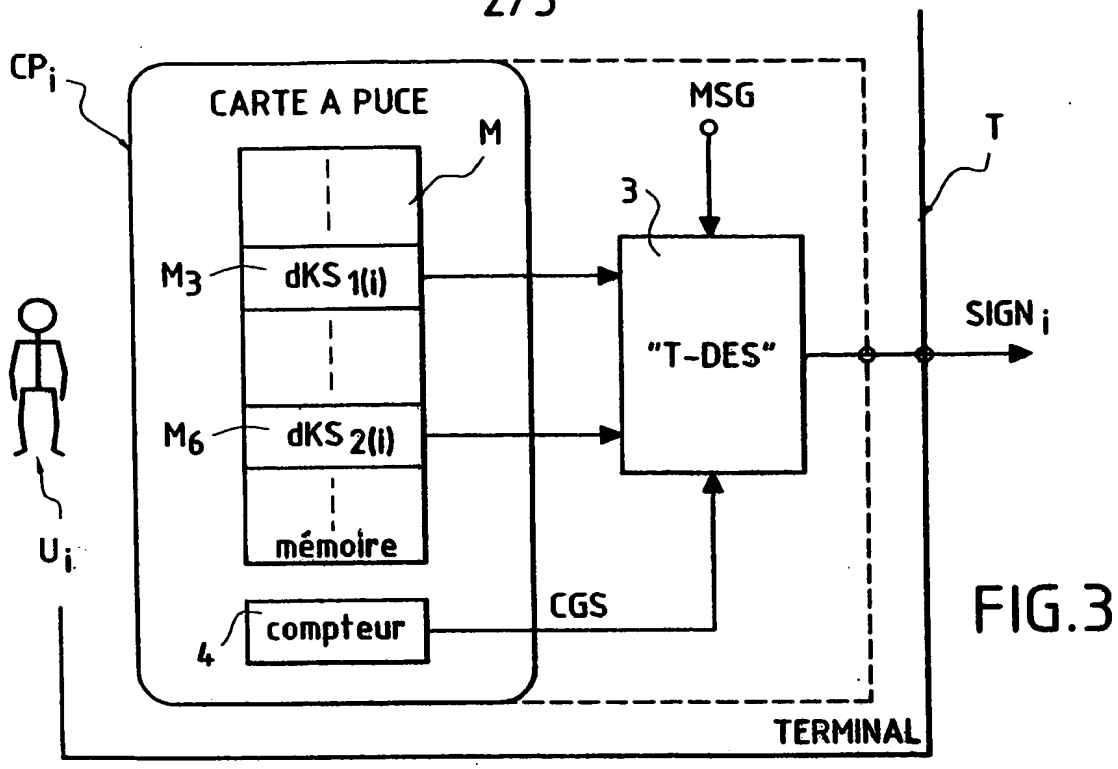

CP i
CARTE A PUCE
M
MSG
T
3
M3
dKS 1(i)
M6
dKS 2(i)
mémoire
"T-DES"
SIGN i
U i
4
compteur
CGS
TERMINAL

FIG.3

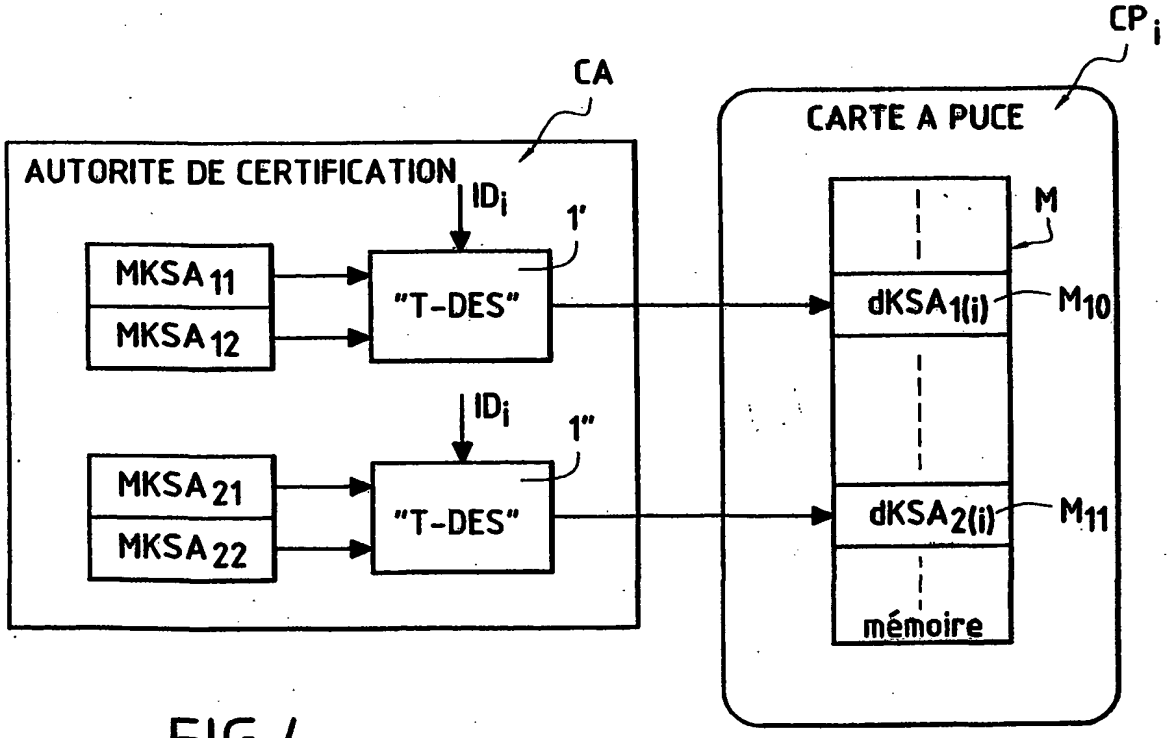

CP i
CA
AUTORITE DE CERTIFICATION
ID i
1'
MKSA 11
MKSA 12
"T-DES"
ID i
1"
MKSA 21
MKSA 22
"T-DES"
CARTE A PUCE
M
dKSA 1(i)
M10
dKSA 2(i)
M11
mémoire

FIG.4

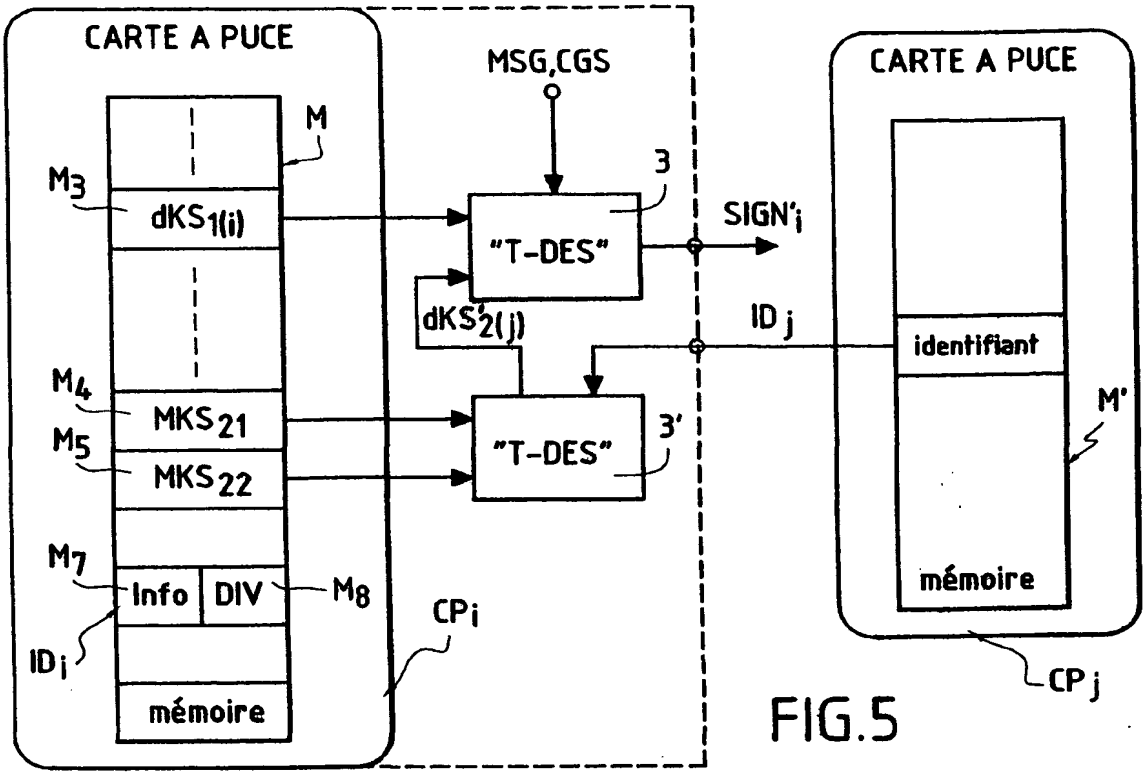


FIG.5

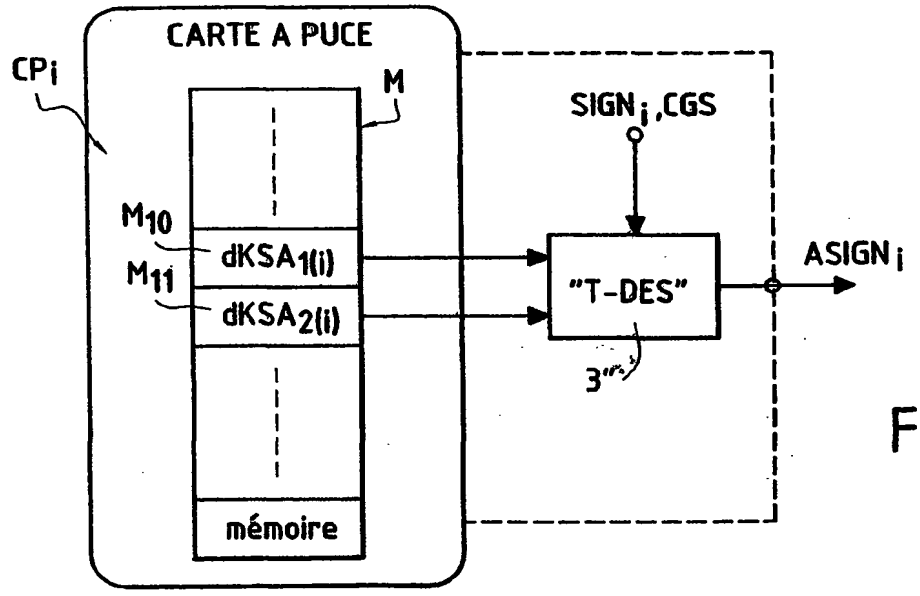


FIG.6

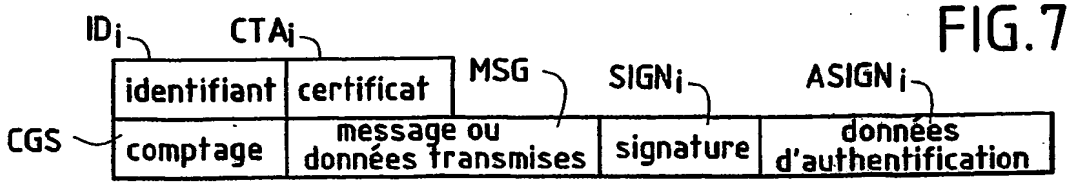


FIG.7

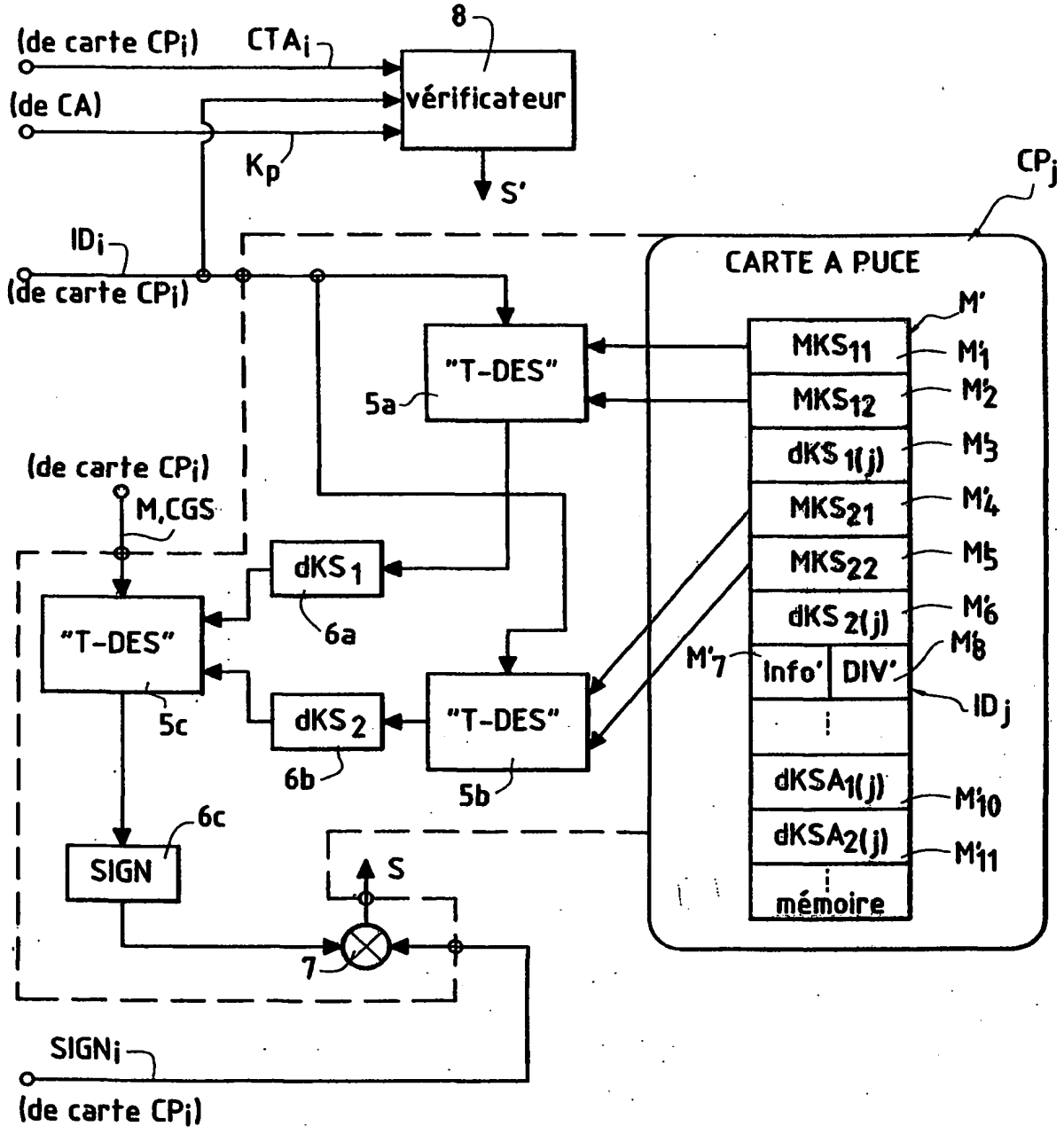
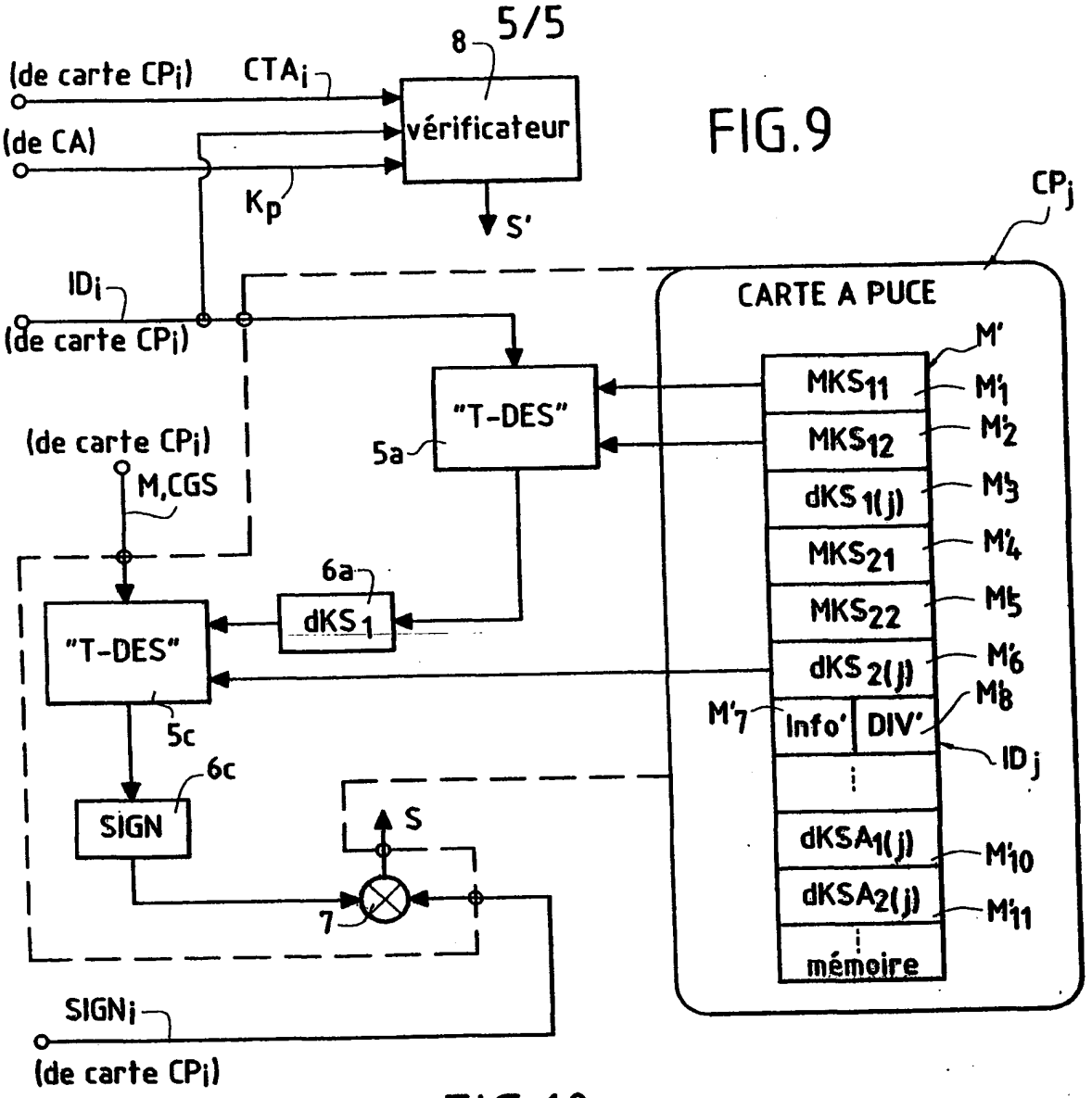

(de carte CPi)
CTAi
8
vérificateur
(de CA)
Kp
S'
CPj
IDi
(de carte CPi)
CARTE A PUCE
M'
"T-DES"
5a
MKS11
M'1
MKS12
M'2
dKS 1(j)
M'3
MKS21
M'4
MKS22
M'5
dKS 2(j)
M'6
M'7
Info'
DIV'
M'8
IDj
dKSA1(j)
M'10
dKSA2(j)
M'11
mémoire
(de carte CPi)
M,CGS
dKS1
6a
"T-DES"
5c
dKS2
6b
"T-DES"
5b
6c
SIGN
S
7
SIGNi
(de carte CPi)

FIG.8


8
(de carte CPi)
CTAi
(de CA)
vérificateur
Kp
S'
FIG.9
CPj
CARTE A PUCE
IDi
(de carte CPi)
M'
MKS11
M'1
"T-DES"
5a
MKS12
M'2
(de carte CPi)
dKS1(j)
M'3
M,CGS
MKS21
M'4
6a
MKS22
M'5
dKS1
"T-DES"
dKS2(j)
M'6
M'7
Info'
DIV'
M'8
IDj
5c
6c
SIGN
S
7
dKSA1(j)
M'10
dKSA2(j)
M'11
mémoire
SIGNi
(de carte CPi)

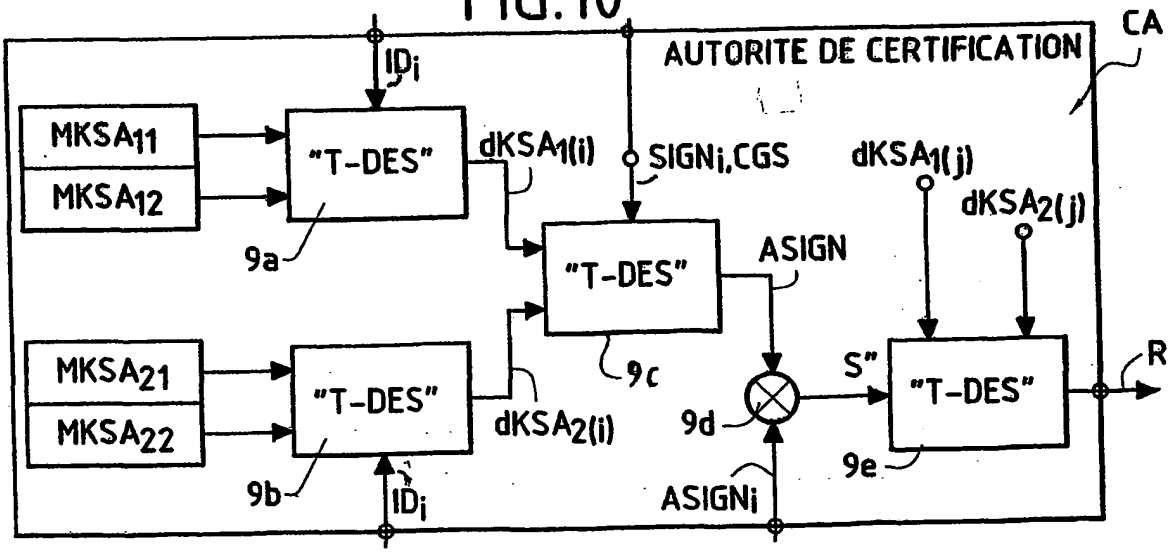


FIG.10
CA
AUTORITE DE CERTIFICATION
IDi
MKSA11
MKSA12
"T-DES"
dKSA1(i)
SIGNi,CGS
dKSA1(j)
dKSA2(j)
9a
"T-DES"
ASIGN
MKSA21
MKSA22
"T-DES"
9c
S"
"T-DES"
R
dKSA2(i)
9d
9b
IDi
ASIGNi
9e

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 01/02720

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
WPI Data, EPO-Internal, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 820 169 A (SCHLUMBERGER IND SA) 21 January 1998 (1998-01-21) abstract column 5, line 1 - line 25; figure 2	1,12,14

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
6 December 2001	13/12/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax (+31–70) 340–3016	Holper, G

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/FR 01/02720

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0820169 A	21-01-1998	FR 2751154 A1	16-01-1998
		EP 0820169 A2	21-01-1998
		JP 10171759 A	26-06-1998
		SG 65664 A1	22-06-1999
		US 5991404 A	23-11-1999

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 01/02720

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
WPI Data, EPO-Internal, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP 0 820 169 A (SCHLUMBERGER IND SA) 21 janvier 1998 (1998-01-21) abrégé colonne 5, ligne 1 - ligne 25; figure 2	1,12,14

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
6 décembre 2001	13/12/2001

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/FR 01/02720

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0820169 A	21-01-1998	FR 2751154 A1	16-01-1998
		EP 0820169 A2	21-01-1998
		JP 10171759 A	26-06-1998
		SG 65664 A1	22-06-1999
		US 5991404 A	23-11-1999